UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/523,760	01/30/2006	Joseph E McIsaac	081893-0102	7549

48329 7590 10/01/2009

FOLEY & LARDNER LLP
111 HUNTINGTON AVENUE
26TH FLOOR
BOSTON, MA 02199-7610

EXAMINER	
WRIGHT, BRYAN F	

ART UNIT	PAPER NUMBER
2431	

MAIL DATE	DELIVERY MODE
10/01/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/523,760	MCISAAC ET AL.	
	Examiner	Art Unit	
	BRYAN WRIGHT	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *15 June 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-95* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-95* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *6/15/2009*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 6/15/2009 has been entered. Claims 1-4, 23-24, 31, 36, 59, 68, 73, and 87 are amended. Claims 1-95 are pending.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

2. Claims 31-95 are rejected under 35 U.S.C. 102(b) as being anticipated by Hall (US Patent No. 5,930,479 cited from IDS).

3. As to claim 31, Hall teaches a method for selectively allowing or denying communication access by other users coupled to an electronic communication network electronic communications network, comprising the steps of:

receiving an inbound message over the electronic communications network from a sender [fig. 2], where the inbound message includes an identifier associated with a sender and an identifier associated with a recipient [1118, 1126, fig. 11];

and determining one of at least three security states (i.e., channel classes) associated with the inbound message (col. 5, lines 50-67), where a first security state is indicative of allowing delivery of the inbound message to the user (i.e., Hall teaches a public channel [col. 7, lines 1-5]), a second security state is indicative of denying delivery of the inbound message to the user (i.e., Hall teaches send - only (channel class 0) is permanently closed to incoming email [col. 6, lines 60-62]), a third security state is indicative of conditionally allowing delivery of the message to the user (i.e., Hall teaches a private channel (class 1) for which a user expect one or a limited number on that particular channel [col. 6, lines 65-67]), each of the at least three security states (i.e., channel classes) are associated with the sender identifier and the recipient identifier included in the inbound message (i.e., Hall teaches channel classes associated with a sender and receiver [col. 11, lines 1-21]).

4. As to claim 32, Hall teaches a method where determining one of the at least three security states (i.e., channel classes) includes determining (i.e., look up) if the recipient identifier matches one of a plurality of proxy identifiers (i.e., Hall teaches a channel id comparison among a plural channel ids contained in a file [col. 11, lines 45- 50]).

5. As to claim 33, Hall teaches a method further comprising: prior to delivery, replacing each reference to the recipient identifier in the message with an identifier associated with the user if the recipient identifier matches one of a plurality \of proxy identifiers [fig. 10C, fig. 10D, fig. 10E].

6. As to claim 34, Hall teaches a method where determining one of the at least three security states (i.e., channel classes) includes determining if the sender identifier matches one of a plurality of sender identifiers (col. 11, lines 35-45).

7. As to claim 35, Hall teaches a method where the recipient identifier is a proxy identifier (i.e., channel id) that is substantially absent content that identifies said user (col. 12, lines 10-25).

8. As to claim 36, Hall teaches a method where the identifiers are e-mail addresses (1126, fig. 11).

9. As to claim 37, Hall teaches a method where detecting the second security state (i.e., channel class 0) initiates sending a reply message to the sender to report the delivery denial (i.e., Hall teaches send - only (channel class 0) is permanently closed to incoming email [col. 6, lines 60- 62]) Hall teaches sending a "No Permission" message [610, fig. 6]).

10. As to claim 38, Hall teaches a method where detecting the second security state initiates (i.e., channel class 0) sending a reply message to the sender that reports the delivery denial (i.e., Hall teaches send - only (channel class 0) is permanently closed to incoming email [col. 6, lines 60-62] Hall teaches sending a "No Permission" message [610, fig. 6]), where the reply message includes a proxy identifier associated with the user for sending a future message [610, fig. 6].

11. As to claim 39, Hall teaches a method where detecting the third security state associates an alert indicator (i.e., channel class 1) with the message (i.e., Hall teaches a private channel (class 1) for which a user expect one or a limited number on that particular channel [col. 6, lines 65-67; col .11, lines 1-6]).

12. As to claim 40, Hall teaches a method where the alert indicator includes a flag (i.e., channel classes [0,1,2]) that is associated with the message (col. 11, lines 1-21).

13. A to claim 41, Hall teaches a method where the third security state is triggered if the message is a response to a message previously sent by the user to the sender [col. 11, lines 1-5].

14. As to claim 42, Hall teaches a method where the third security state is triggered if the recipient identifier included in the message is a proxy identifier (i.e., channel id) generated by the user and is absent from the plurality of proxy identifiers (i.e., Hall teaches a private channel (class 1) for which a user expect one or a limited number on that particular channel [col. 6, lines 65-67]).

15. As to claim 43, Hall teaches a method where the third security state is triggered if the recipient identifier and the sender identifier include the same network domain (i.e., host) (i.e., Hall teaches a channelized address specifying a host name (i.e., domain name) [col. 5, lines 45-50; 200, fig. 3]).

16. As to claim 44, Hall teaches a method where the recipient identifier (i.e., channel classes) is a proxy identifier assigned to the user for a period of time (i.e., Hall teaches user defined channel class capability [col. 7, lines 10 -20]).

17. As to claim 45, Hall teaches a system where at least one of the generated proxy identifiers (i.e., channel id) associated with said user is substantially absent content that identifies said user (col. 12, lines 15-25]).

18. As to claim 46, Hall teaches a system where at least one of the generated proxy Identifiers (i.e., channel classes) associated with said user is valid for a predefined time period (i.e., Hall teaches user defined channel class capability [col. 7, lines 10 -20]).

19. As to claim 47, Hall teaches a system further comprising: a database (i.e., UCDB) configured to store the plurality of proxy identifiers (col. 10, lines 55-67).

20. As to claim 48, Hall teaches a system the database (i.e., UCDB) includes an entry that stores data that represents a contact name associated with said user, a proxy identifier assigned to said user, and the security state associated with the proxy address (col. 10, lines 55-67).

21. As to claim 49, Hall teaches a system where the processor attempts to match said sender identifier with a least one of a plurality of identifiers associated with the user (col. 12, lines 15-25).

22. As to claim 50, Hall teaches a system where the processor determines the security state (i.e., channel classes) associated with said user that overrides the security state associated with the message [col. 7, lines 10-30].

23. As to claim 51, Hall teaches a system where the processor determines if said recipient identifier matches one of said plurality of proxy identifiers associated with said user (608, fig. 6).

24. As to claim 52, Hall teaches a system where the gate initiates sending a reply message to said sender to report denying (i.e., reject) transfer of said message (610, fig. 6).

25. As to claim 53, Hall teaches a system where the gate initiates sending a reply message to said sender to report denying transfer of said message, wherein said reply message (i.e. "No permission") includes one of said plurality of proxy identifiers associated with said user (610, fig. 6).

26. As to claim 54, Hall teaches a system where the processor initiates entering said sender identifier into a database (i.e., UCDB) when access to the user by transferring said message is denied (col. 10, lines 55-67).

27. As to claim 55, Hall teaches a system where the processor determines if said user replied to a previously sent message from said sender to determine whether to transfer said message to said user (i.e., Hall teaches a correspondent address associated with channel id [fig. 4] Hall teaches a correspondent known to the recipient (i.e., received email from correspondent previously) will have a channel id [col. 12, lines 15-25]).

28. As to claim 56, Hall teaches a system where the processor determines if said user initiated generation (i.e. known user) of said recipient identifier to determine whether to transfer said message to said user [604,606, fig. 6].

29. As to claim 57, Hall teaches a system where said user-generated recipient identifier (i.e., channel id) is absent from said plurality of proxy identifiers [609, fig. 6].

30. As to claim 58, Hall teaches a system where if said processor determines that said user-generated recipient identifier is absent, said processor initiates adding said user-generated recipient identifier into said plurality of proxy identifiers (i.e., Hall teaches a first message to recipient [col. 12, lines 55-67]).

31. As to claim 59, Hall teaches a system where if said message is transferred to said user, said processor initiates removing (i.e., strip off) from any reference to said recipient identifier from said message (col. 12, lines 35-40).

32. As to claim 60, Hall teaches a system where if said message is transferred to said user, said processor initiates adding a reference to an identifier associated with the recipient in said message (fig. 10C, fig. 10D, fig. 10E).

33. As to claim 61, Hall teaches a system where if said first security state is detected (i.e., Hall teaches a public channel [col. 7, lines 1-5]), the gate allows transfer of said inbound to said user (col. 12, lines 22-25).

34. As to claim 62, Hall teaches a system where if said second state is detected, the gate blocks transfer of said inbound message to said user (i.e., Hall teaches send - only (channel class 0) is permanently closed to incoming email [col. 6, lines 60- 62]).

35. As to claim 63, Hall teaches a system where said predetermined criteria includes the user responding to a previously sent message from said sender (i.e., Hall teaches a correspondent address associated with channel id [fig. 4] Hall teaches a correspondent known to the recipient (i.e., received email from correspondent previously) will have a channel id [col. 12, lines 15-25]).

36. As to claim 64, Hall teaches a system where said previously sent message includes the sender identifier (col. 12, lines 15-25).

37. As to claim 65, Hall teaches a system where the predetermined criteria includes the processor matching the sender identifier to one of a plurality of identifiers (fig. 4).

38. As to claim 66., Hall teaches a system where the predetermined criteria includes the processor matching the recipient identifier to one of the plurality of proxy Identifiers (col. 12, lines 15-20).

39. As to claim 67, Hall teaches a system where the predetermined criteria includes the processor determining that the recipient identifier and the sender identifier are associated with the same network domain (i.e.host) (i.e., Hall teaches a channelized address specifying a host name (i.e., domain name) [col. 5, lines 45-50; 200, fig. 3]).

40. As to claim 68, Hall teaches a system for selectively allowing or denying communication access by other users coupled to an electronic communication network to a user coupled to the electronic communications network, comprising: a receiver configured to receive an inbound message over the electronic communications network from a sender (602, fig. 6),

wherein the inbound message includes an identifier of the sender and an identifier of the recipient; and a processor configured to determine one of at least three security states (i.e., channel classes) associated with the inbound message (col. 5, lines 50- 67), where a first security state is indicative of allowing delivery of the inbound message to the user (i.e., Hall teaches a public channel [col. 7, lines 1-5]), a second security state is indicative of denying delivery of the inbound message to the user (i.e., Hall teaches send - only (channel class 0) is permanently closed to incoming email [col. 6, lines 60-62]),

a third security state is indicative of conditionally allowing delivery of the message to the user (i.e., Hall teaches a private channel (class 1) for which a user expect one or a limited number on that particular channel [col. 6, lines 65-67]),

each of the at least three security states (i.e., channel classes) are associated with the sender identifier and the recipient identifier included in the inbound message (i.e., Hall teaches channel classes associated with a sender and receiver [col. 11, lines 1-21]).

41. As to claim 69, Hall teaches a system where the processor determines if the recipient identifier matches one of a plurality of proxy identifiers to determine one of the at least three security states (i.e., Hall teaches checking channel id exist in recipient file [col. 12, lines 15-20] Hall teaches channel classes [0,1 ,.2] representative of how the mail will be treated [col. 6, lines 50-67]).

42. As to claim 70, Hall teaches a system where prior to delivery, the processor is configured to replace each reference to the recipient identifier in the message with an identifier of the user if the recipient identifier matches one of a plurality of proxy identifiers (fig. 10C, fig. 10D, fig. 10E).

43. As to claim 71, Hall teaches a system where the processor is configured to determine if the sender identifier (i.e., key) matches (i.e., locating) one of a plurality of sender identifiers (i.e., Hall teaches locating key in UCDB [col. 15, lines 25-35]).

44. As to claim 72, Hall teaches a system where the recipient identifier is a proxy identifier (i.e., channel id) that is substantially absent content that identifies said user (col. 11, lines 28-33).

45. As to claim 73, Hall teaches a system where the sender identifier is an e-mail address and the recipient identifier is an email address (1126, fig. 11).

46. As to claim 74, Hall teaches a system where when the second security state is detected, the processor initiates sending a reply message to the sender to report the delivery denial (i.e., Hall teaches send - only (channel class 0) is permanently closed to incoming email [col. 6, lines 60-62] Hall teaches sending a "No Permission" message [610, fig. 6]).

47. As to claim 75, Hall teaches a system where when the second security state is detected, the processor initiates sending a reply message to the sender to report the delivery denial, where the reply message includes a proxy identifier to send a future message (i.e., Hall teaches send - only (channel class 0) is permanently closed to incoming email [col. 6, lines 60-62] Hall teaches sending a "No Permission" message [610, fig. 6]).

48. As to claim 76, Hall teaches a system where when the third security state is detected, an alert indicator is associated (i.e., channel class 1) with the message (i.e., Hall teaches a private channel (class 1) for which a user expect

one or a limited number on that particular channel [col. 6, lines 65-67;col .11, lines 1-6]).

49. As to claim 77, Hall teaches a system where the alert indicator includes a flag (i.e., channel class designation [0,1, 2]) that is associated with the message (col. 11, lines 1-20).

50. As to claim 78, Hall teaches a system where the third security state is triggered if the message is a response to a previously sent message from the user to the sender (i.e., Hall teaches a private channel (class 1) for which a user expect one or a limited number on that particular channel [col. 11, lines 1-5]).

51. As to claim 79, Hall teaches a system where the third security state is triggered if the recipient identifier is a proxy identifier generated by the user and is absent from a plurality of proxy identifiers associated with the user that are stored in a database (i.e., Hall teaches a private channel (class 1) for which a user expect one or a limited number on that particular channel [col. 6, lines 65-67]).

52. As to claim 80, Hall teaches a system where the third security state is triggered (i.e., public channel/channel class 2) if the user identifier and the sender identifier include the same network domain (e.g., anyone can send email)

(i.e., Hall teaches any one of a number of correspondents may send e-mail using the public channel ID [col. 11, lines 10-15]).

53. As to claim 81, Hall teaches a system where the recipient identifier is assigned to the user for a period of time (i.e., Hall teaches user defined channel class capability [col. 7, lines 10-20]).

54. As to claims 82, Hall teaches a computer program product residing on a computer readable medium having a plurality of instructions stored thereon which, when executed by a processor, cause that processor to:

receive an inbound message over a electronic communications network from a sender (602, fig. 6), wherein the inbound message includes an identifier of the sender and an identifier of a recipient; and determine one of at least three security states (i.e., channel classes) associated with the inbound message (col. 5, lines 50-67), where a first security state is indicative of allowing delivery of the inbound message to a user (i.e., Hall teaches a public channel [col. 7, lines 1-5]), a second security state is indicative of denying delivery of the inbound message to the user (i.e., Hall teaches send - only (channel class 0) is permanently closed to incoming email [col. 6, lines 60-62]),

a third security state is indicative of conditionally allowing delivery of the message to the user (i.e., Hall teaches a private channel (class 1) for which a user expect one or a limited number on that particular channel [col. 6, lines 65-67]),

each of the at least three security states are associated with the sender identifier and the recipient identifier included in the inbound message (i.e., Hall teaches channel classes associated with a sender and receiver [col. 11, lines 1-21]).

55. As to claim 83, Hall teaches a computer program product where to determine one of the at least three security states (i.e., channel classes) includes determining if the recipient identifier matches one of a plurality of proxy identifiers (i.e., Hall teaches a channel id comparison among a plural channel ids contained in a file [col. 11, lines 45- 50]).

56. As to claim 85, Hall teaches a computer program product where to determine one of the at least three security states (i.e., channel classes) includes determining if the sender identifier matches one of a plurality of sender identifiers (i.e., Hall teaches a channel id comparison among a plural channel ids contained in a file [col. 11, lines 45- 50]).

57. As to claim 86, Hall teaches a computer program product where the recipient identifier (i.e., channel id) is a proxy identifier that is substantially absent content that identifies said user (col. 12, lines 10-25).

58. As to claim 87, Hall teaches a computer program product where the sender identifier is an e-mail address and the recipient identifier is an e-mail address (1126, fig. 11).

59. As to claim 88, Hall teaches a computer program product further comprising instructions for: upon detecting the second security state (i.e., channel class 0) (i.e., Hall teaches send - only (channel class 0) is permanently closed to incoming email [col. 6, lines 60-62]), sending a reply message to the sender to report delivery denial (i.e., Hall teaches sending a "No Permission" message [610, fig. 6]).

60. As to claim 89, Hall teaches a computer program product further comprising instructions for: upon detecting the second security state (i.e., channel class 0) (i.e., Hall teaches send - only (channel class 0) is permanently closed to incoming email [col. 6, lines 60-62]), sending a reply message to the sender that reports the delivery denial (i.e., Hall teaches sending a "No Permission" message [610, fig. 6]), wherein the reply message includes a proxy address to send a future message.

61. As to claim 90, Hall teaches a computer program product further comprising instructions for: upon detecting the third security state (i.e. user expect one or a limited number), associating an alert indicator (i.e., channel class 1) with the message (i.e., Hall teaches a private channel (class 1) for which a

user expect one or a limited number on that particular channel [col. 11, lines 1-20]).

62. As to claim 91, Hall teaches a computer program product where the alert indicator (i.e., channel class designation [0, 1, 2]) includes a flag that is associated with the message (col. 11, lines 1-20).

63. As to claim 92, Hall teaches a computer program product where the third security state is triggered if the message is a response to a previously sent message from the user to the sender [col. 11, lines 1-5].

64. As to claim 93, Hall teaches a computer program where the third security state (i.e., public channel/channel class 2) is triggered if the recipient identifier in the message is a proxy identifier generated by the user and is absent (i.e., use of public channel ID) from a plurality of proxy identifiers that are associated with the user and stored in a database (i.e., Hall teaches any one of a number of correspondents may send e-mail using the public channel ID [col. 11, lines 10-15] Hall teaches use of public channel ID. Hall teaches correspondents information (i.e., address, channel) in database).

65. As to claim 94, Hall teaches a computer program where the third security state (i.e., public channel/channel class 2) is triggered if the recipient identifier and the sender identifier include the same network domain (e.g., anyone can

send email) (i.e., Hall teaches any one of a number of correspondents may send e-mail using the public channel ID [col. 11, lines 10-15]).

66. As to claim 95, Hall teaches a computer program product where the recipient identifier (i.e., channel classes) is assigned to the user for a period of time (i.e., Hall teaches user defined channel class capability [col. 7, lines 10 - 25]).

Claim Rejections - 35 USC § 103

. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

67. Claim 1-30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hall in view of Katsikas (WO 01/16695 (cited from IDS)).

68. As to claim 1, Hall teaches a method for selectively allowing or denying communication access by other users coupled to an electronic communications network, said user having an associated recipient identifier, comprising the steps of:

generating a plurality of distinct proxy identifiers (i.e., channel id) associated with said user, each of said proxy identifiers (i.e., channel id) having at least three associated security states (i.e., three classes) [col. 6, lines 50-60],

a first of said states being indicative of allowing any other user coupled to said electronic communication network communication access to said user (i.e., Hall teaches a public channel [col. 7, lines 1-5]),

a second of said states being indicative of denying any other user coupled to said electronic communication network communication access to said user (i.e., Hall teaches send - only (channel class 0) is permanently closed to incoming email [col. 6, lines 60-62]),

and a third of said states being conditionally indicative of allowing at least one but fewer than all other user coupled to said electronic communication network communication access to said user if predetermined criteria are met and denying access to said user otherwise (i.e., Hall teaches a private channel (class

1) for which a user expect one or a limited number on that particular channel [col. 6, lines 65-67]);

in response to an inbound message from said electronic communication network including a sender identifier and said recipient identifier, said sender identifier being associated with a sender of said inbound message, transfer (i.e., send) said inbound message to a location associated with one of said proxy identifiers (i.e., channel id) associated with said user (i.e., Hall teaches receiving a message (fig. 6,602). Hall teaches send the message to personal channel agent [fig. 6,612]);

processing (i.e., strips off the channel id) said transferred inbound message to evaluate a security status associated therewith (i.e., Hall teaches the PCA strips off the channel ID from message header information), said security status being related to said sender identifier and said recipient identifier (i.e., Hall teaches a channel class designation for which classifies a sender and recipient communication [col. 6, lines 60- 67]);

allowing communication access for said transferred message to said user when said security status corresponds to said third state and meets one or more of said predetermined criteria (i.e., channel classes) at least partially related to said security status of said one proxy identifier (i.e., channel id), and denying communication access for said transferred message to said user otherwise (i.e., Hall teaches a private channel (class 1) for which a user expect one or a limited number on that particular channel [col. 6, lines 65-67]).

Hall does not expressly teach:

controlling communication access for said transferred message to said user by: i. allowing communication access for said transferred message to said user when said security status corresponds to said first state; denying communication access for said transferred message to said user when said security status corresponds to said second state.

However, the feature of controlling communication access for email communication based on predetermined rules for distinct participating network users is well known in the art and would have been an obvious modification of the system disclosed by Hall as introduced by Katsikas. Katsikas discloses:

controlling communication access for said transferred message to said user by (to provide communication access [abstract]): allowing communication access for said transferred message to said user when said security status corresponds to said first state (to provide predetermined rules for controlling message communication between distinct network user [pg. 5, lines 15-25]); denying communication access for said transferred message to said user when said security status corresponds to said second state.

Therefore, given the teachings of Katsikas, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Hall by employing the well known feature communication control using predetermine communication rules disclosed above by Katsikas,

thereby enhancing the filtering of Spam messages within a network [pg. 10, 19-30].

69. As to claim 2, Hall teaches a method where said identifiers are e-mail address and said recipient identifier is an email address (1126, fig. 11).

70. As to claim 3, Hall teaches a system for selectively allowing or denying communication access by other users coupled to an electronic communication network to a user coupled to the electronic communications network, said user having an associated recipient identifier, comprising:

generating a plurality of distinct proxy identifiers (i.e., channel id) associated with said user, each of said proxy identifiers having at least three associated security states (i.e., channel classes 0,1,2),

a first of said states being indicative of allowing any other user coupled to said electronic communication network communication access to said user (i.e., Hall teaches a public channel [col. 7, lines 1-5]),

a second of said states being indicative of denying any other user coupled to said network access to said user (i.e., Hall teaches send - only (channel class 0) is permanently closed to incoming email [col. 6, lines 60-62]),

and a third of said states being conditionally indicative of allowing at least one but fewer than all other users coupled to said electronic communication network communication access to said user if predetermined criteria are met and denying access to said user otherwise (i.e., Hall teaches a private channel (class

1) for which a user expect one or a limited number on that particular channel [col. 6, lines 65-67]);

in response to an inbound message from said electronic communication network including a sender identifier and said recipient identifier, said sender identifier being associated with a sender of said inbound message, to transferring (i.e., send) said inbound message to a location associated with one of said proxy identifiers (i.e., channel id) associated with said user (i.e., Hall teaches receiving a message (fig. 6,602). Hall teaches send the message to personal channel agent [fig. 6,612]);

processing said transferred inbound message to evaluate a security status associated therewith, said security status being related to said sender identifier and said recipient identifier (col. 11, lines 1-26), and

allowing communication access for said transferred message to said user when said security status corresponds to said third state end meets one or more of said predetermined criteria at least partially related to said security states of said one proxy identifier, and denying communication access for said transferred message to said user otherwise (i.e., Hall teaches a private channel (class 1) for which a user expect one or a limited number on that particular channel [col. 6, lines 65-67]),

Hall does not expressly teach:

controlling communication access for said transferred message to said user by: allowing communication access for said transferred message to said

user when said security status corresponds to said first state; denying communication access for said transferred message to said user when said security status corresponds to said second state.

However, the feature of controlling communication access for email communication based on predetermined rules for distinct participating network users is well known in the art and would have been an obvious modification of the system disclosed by Hall as introduced by Katsikas. Katsikas discloses:

controlling communication access for said transferred message to said user by (to provide communication access [abstract]): allowing communication access for said transferred message to said user when said security status corresponds to said first state (to provide predetermined rules for controlling message communication between distinct network user [pg. 5, lines 15-25]); denying communication access for said transferred message to said user when said security status corresponds to said second state.

Therefore, given the teachings of Katsikas, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Hall by employing the well known feature communication control using predetermine communication rules disclosed above by Katsikas, thereby enhancing the filtering of Spam messages within a network [pg. 10, 19-30].

71. As to claim 4, Hall teaches a system where said identifiers are e-mail address and said recipient identifier is an e-mail address (1126, fig. 11).

72. As to claim 5, Hall teaches a method where at least one of the generated proxy identifiers (i.e., channel id) associated with said user is substantially absent content that identifies said user (col. 11, lines 28-33).

73. As to claim 6, Hall teaches a method where at least one of the generated proxy identifiers (i.e., channel classes) associated with said user is valid for a predefined time period (i.e., Hall teaches user defined channel class capability [col. 7, lines 10 -20]).

74. As to claim 7, Hall teaches a method where the plurality of proxy identifiers (i.e., channel id) are stored in a database (fig. 11).

75. As to claim 8, Hall teaches a method where an entry in the database includes data representing a contact name associated with said user (1118, fig. 11), a proxy address assigned to said user (1126, fig. 11), and the security state associated with the proxy address (1106, 1108, 1110, fig. 11).

76. As to claim 9, Hall teaches a method where processing said transferred inbound message includes attempting to match (i.e., look up) said recipient identifier with at least one of the plurality of proxy identifiers (i.e., channel id)

associated with said user (i.e., Hall teaches a comparison match for which a channel id is selectively compared among a plurality [col. 11, lines 35-55]).

77. As to claim 10, Hall teaches a method where processing said transferred inbound message includes attempting to match said sender identifier with at least one of a plurality of identifiers (i.e., channel id) associated with contacts of the user (col. 11, lines 4O- 53).

78. As to claim 11, Hall teaches a method where processing said transferred inbound message includes determining the security state (i.e., channel classes) associated with said user (i.e., Hall teaches channel classes [0,1,2] associated with a correspondents address. Hall teaches the channel classes indicate how sender and recipient are to communicate [col. 11, lines 1-20]).

79. As to claim 12, Hall teaches a method where denying transfer of said message to said user includes sending a reply message to said sender (606, fig. 6).

80. s to claim 13, Hall teaches a method where denying transfer of said message to said user includes sending a reply message to said sender (610, fig. fig.6), where said reply message includes one of said plurality of proxy identifiers (i.e., channel id) associated with said user (i.e., Hall teaches evaluating a

channel ID to determine if the channel id exist [608, fig. 6] Hall teaches sending a message to sender [610, fig.6]).

81. As to claim 14, Hall teaches a method where denying (i.e., reject) transfer of said message to said user includes generating a proxy identifier (i.e., channel id) associated with said user and sending a reply message to said sender (i.e., Hall teaches sending a "no permission message" to sender for which said sender is associated with a channel id [1126, fig. 11]), where said reply message (i.e., "no permission message" [610, fig. 6]) includes the generated proxy identifier (i.e., channel id) associated with said user [fig. 11].

82. As to claim 15, Hall teaches a method where denying (i.e., no correspondent key entry) transfer of said message to said user includes entering said sender identifier into a database (i.e., UCDB) (col. 10, lines 55-67).

83. As to claim 16, Hall teaches a method where allowing transfer of said message to said user includes determining if said user replied to a message previously sent from said sender (i.e., Hall teaches a correspondent address associated with channel id [fig. 4] Hall teaches a correspondent known to the recipient (i.e., received email from correspondent previously)will have a channel id [col. 12, lines 15-25]).

84. As to claim 17, Hall teaches a method where allowing transfer of said message to said user includes determining if said user initiated generation of a proxy identifier included in the message (i.e., Hall teaches determining if known user [606, fig. 6] Hall further teaches determining if channel id exist [col. 12, lines 15-25]).

85. As to claim 18, Hall teaches a method where said user-generated proxy identifier absent (i.e., unknown user) from said plurality of proxy identifiers (col. 12, lines 15-25).

86. As to claim 19, Hall teaches a method further comprising the step: if said user- generated proxy identifier is absent from said plurality of proxy identifiers, adding (i.e., enter) said user generated proxy identifier to said plurality of proxy identifiers (i.e., Hall teaches determining if this a first-time sender. Hall teaches the action to capture correspondent information [col. 12, lines 55-65]).

87. As to claim 20, Hall teaches a method where allowing transfer of said message to said user includes removing (i.e., strip off) reference to said user-generated proxy identifier in said message (col. 12, lines 35-40).

88. As to claim 21, Hall teaches a method where allowing transfer of said message to said user includes removing (i.e., strip off) reference to said user-

generated proxy identifier in said message and adding an e-mail address associated with said user to said message (col. 12, lines 35-40).

89. As to claim 22, Hall teaches a method where processing said inbound message includes removing (i.e., separate) reference to said recipient identifier (i.e., channel id) included in said message (i.e., Hall teaches processing a message involves employing a process of separation [col. 11, lines 40-45]).

90. As to claim 23, Hall teaches a method where said first state that is indicative of allowing any other user coupled to said electronic communication network communication access to said user, includes allowing transfer of a message from said other user to said user (i.e., Hall teaches a public channel [col. 7, lines 1-5]).

91. As to claim 24, Hall teaches a method where said second state that is indicative of denying any other user coupled to said electronic communication network communication access to said user, includes blocking transfer of a message from said any other coupled to said user (i.e., Hall teaches send - only (channel class 0) is permanently closed to incoming email [col. 6, lines 60-62]).

92. As to claim 25, Hall teaches a method where said predetermined criteria includes the user previously responding to a message previously sent by the sender (i.e., Hall teaches a correspondent address associated with channel id

[fig. 4] Hall teaches a correspondent known to the recipient (i.e., received email from correspondent previously) will have a channel id [col. 12, lines 15-25]).

93. As to claim 26, Hall teaches a method where said previously sent message includes said sender identifier (i.e., key) (i.e., Hall teaches a previous message sent by sender containing a key for which could be used to determine the sender to be legitimate [col. 15, lines 15-25]).

94. As to claim 27, Hall teaches a method where one of the predetermined criteria includes the sender identifier (i.e., key) matching (i.e., locating) one of a plurality of identifiers (i.e., Hall teaches locating key in UCDB [col. 15, lines 25-35]).

95. As to claim 29, Hall teaches a method where one of the predetermined criteria includes the recipient identifier matching one of the plurality of proxy identifiers (i.e., Hall teaches a comparison match for which a channel id is selectively compared among a plurality [col. 11, lines 35-55]).

96. As to claim 30, Hall teaches a method where one of the predetermined criteria includes both the recipient identifier and the sender identifier are associated with the same network domain (i.e., host) (i.e., Hall teaches a channelized address specifying a host name (i.e., domain name) [col. 5, lines 45-50; 200, fig. 3]).

Response to Arguments

Applicant's arguments with respect to claims 1-95 have been considered but are moot in view of the new ground(s) of rejection. With regards to applicant's argument of " Hall only rejects the message based on either the recipient's address, in step 604 and 606, or the channel identifier, in step 608 and 610", the Examiner contends that Hall teaches the sender address is translated into a proxy identifier [par. 20 and 21]. The proxy identifier (e.g., senders address) is then used to make the proper in-bound message preparation according to security states [par. 139].

With regards to applicant's argument of "...In contrast, all of Applicant's claims use both the sender's address and the recipient's address to determine the security state", the Examiner contends applicant formally recognizes that Hall teaches the use of the recipient address as means to determine security state (e.g., allow or deny). See applicant's argument page 20, filed 6/15/2009. Additionally, the Examiner contends Hall teaches that the sender address is translated into a proxy identifier [par. 20 and 21]. Upon translating the sender address to the proxy identifier (e.g., sender address), the proxy identifier is used in the security determination process [par. 139].

Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to BRYAN WRIGHT whose telephone number is

(571)270-3826. The examiner can normally be reached on 8:30 am - 5:30 pm Monday -Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William Korzuch can be reached on (571) 272-7589. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/BRYAN WRIGHT/
Examiner, Art Unit 2431

/William R. Korzuch/
Supervisory Patent Examiner, Art Unit 2431